SOLUTION BRIEF

NETWORK DDOS PROTECTION

Next-generation Threat Protection for Highly Available Services

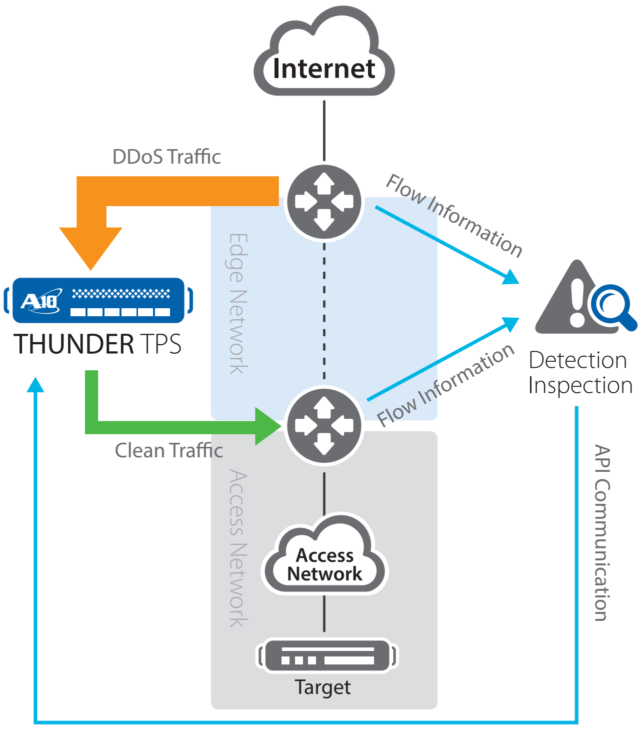
The Service Availability Challenge

Today, service providers such as cloud providers, Web hosting services, Internet Service Providers (ISPs) as well as large enterprises, require an environment that is highly available and secure, as the Internet is the main, if not the only way to channel an organization's services to its customers. Over the last few years, distributed denial of service (DDoS) attacks have grown dramatically in frequency, size and complexity. While organizations have existing security strategies in place that mitigate a range of existing security threats, they are clearly not prepared to address this new breed of DDoS attacks, which leverage large distributed "botnet" networks of compromised "zombie" machines to simultaneously launch attacks using compliant protocols that are very difficult to detect and even harder to mitigate. It is clear that additional solutions are needed to complement existing security infrastructure in a layered defense model.

Service availability is at risk: The Internet is a shared medium, and malicious DDoS attacks have increased rapidly in the last few years, originating from and targeted at many different locations. Attacks may be generated by ideological groups (hacktivism) for political reasons, by organized criminal syndicates (cybercrime) for extortion and theft, or by foreign military intelligence agencies. Today, DDoS attacks can also be generated by novice hackers without much expertise to take anyone or any service off the Internet. When an organization's services are unavailable to its customer base, it can quickly result in revenue loss, customer frustration and dissatisfaction, and damaged brand reputation.

DDoS is a big number issue: The intent of a DDoS attack is to render a service unavailable to legitimate users. To create an effective DDoS attack, many infected computers, known as zombies, or bots, are controlled remotely to send malicious traffic to a victim in unison. Leveraging the large number of zombies inside these botnets, traffic volume towards the victim quickly grows to a massive scale. Depending on the DDoS attack type, a victim's Internet connection can simply become saturated, network security services can become overwhelmed trying to inspect the intense volume of zombie traffic, or application servers can become exhausted trying to respond to the many botnet requests.

Solutions are not easy to integrate: Deploying DDoS protection services in an existing network can be challenging; they may introduce choke points and increase latency for the services they are trying to protect. Service providers often deal with many different network architectures and have invested in a existing security strategy. Network operators want to stick to their choice of network analysis and security detection solutions, and require DDoS mitigation devices that can integrate with and complement solutions from different vendors.

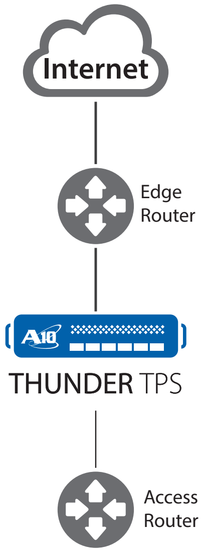


TPS in asymmetric mode

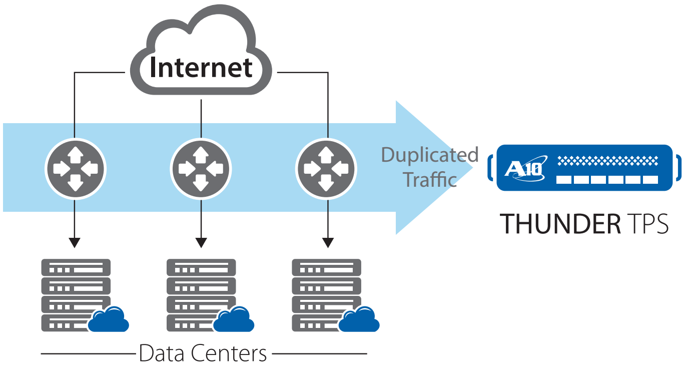
A10 Thunder TPS – The Next-generation in Threat Protection

The A10 Thunder™ Threat Protection System (TPS) product line provides high-performance, network-wide protection against DDoS attacks, and it ensures service availability against a variety of volumetric, protocol, resource and other sophisticated application attacks.

- **Multi-level DDoS protection ensures service availability:** Thunder TPS protects against multiple classes of attack vectors, including volumetric, protocol, resource and advanced application-layer attacks, which are quickly detected and mitigated to prevent a service from becoming unavailable. A baseline of normal traffic can be established, so traffic anomalies are quickly recognized. In addition, customized actions can be taken against advanced application-layer (L7) attacks as needed with our aFleX® deep-packet inspection (DPI) scripting technology.
- **Performance scalability meets growing attack scale:** With DDoS mitigation capacity ranging from 38 to 155 Gbps, (and up to 1.2 Tbps in a cluster), Thunder TPS ensures that the largest DDoS attacks can be handled effectively. Each Thunder TPS model is equipped with high-performance field programmable gate array (FPGA)-based Flexible Traffic Acceleration (FTA) technology, to immediately detect and mitigate over 30 common attack vectors in hardware (SYN cookies, for example) without impact to the core system general-purpose CPUs. More complex application-layer (L7) attacks (HTTP, SSL, DNS, etc.) are processed by the latest Intel Xeon CPUs, so that performance scaling can be maintained by distributing multi-vector detection and mitigation functions across optimal system resources to mitigate application-layer attacks such as Slowloris.
- **Broad deployment flexibility:** With flexible deployment models for in- and out-of-band operations, and routed or transparent operation modes, Thunder TPS can easily be integrated into any network architecture, of any size. And with our open RESTful API, aXAPI®, Thunder TPS enables integration to your custom or third-party detection solutions. In addition to processing large network traffic volumes, Thunder TPS maintains detailed statistics or telemetry of all traffic, and can share via sFlow with your network analytics to enhance network traffic visibility. Thunder TPS also provides robust support for best-in-class third-party security service integration with more than 120 million rules that can be imported, and can be utilized in blacklists, whitelists and other rule sets.



TPS in inline mode



TPS in out-of-band mode

Summary

The A10 Thunder TPS product line offers a variety of solutions that solve the DDoS attack challenges and problems faced by today's service providers and large enterprises. Thunder TPS protects network infrastructure and allows existing security solutions to scale against unexpected, large-scale DDoS attacks, providing network operators detailed network insight and peace of mind.

To ensure that your data center resources are used efficiently, Thunder TPS provides many high-performance and sophisticated features, in the most efficient hardware form factors, to mitigate the largest and most complex DDoS attacks. The combination of high performance in a small form factor results in lower OPEX through significantly lower power usage, less rack space, and reduced cooling requirements.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: 19103-EN-03 Feb 2014

Worldwide Offices

North America
sales@a10networks.com

Europe
emea_sales@a10networks.com

South America
brazil@a10networks.com

Japan
jinfo@a10networks.com

China
china_sales@a10networks.com

Taiwan
taiwan@a10networks.com

Korea
korea@a10networks.com

Hong Kong
HongKong@a10networks.com

South Asia
SouthAsia@a10networks.com

Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.